


signing key expiry data to a plurality of clients, that are selectable on a per client basis wherein the digital signature key pairs are not shared among users;

digitally storing both selected public key expiry data and selected private key expiry data for association with a new digital signature key pair; and

associating the stored selected expiry data with a new digital signature key pair to effect a transition from an old digital signature key pair to a new digital signature key pair

determining whether a digital signature key pair update request has been received from a client unit;

receiving a new digital signature key pair from the client unit in response to the digital signature key pair update request; and

wherein the step of associating the stored selected expiry data includes creating a new digital signature certificate containing the selected public key expiry data selected for the client that generated the digital signature key pair update request.

2. (Once Amended) The method of claim 1 wherein the selectable expiry data is digital signature certificate lifetime data for variably setting a lifetime end date for a digital signature certificate.

3. (Once Amended) The method of claim 1 further including the step of providing variable update privilege control on a per client basis to the multi-client manager unit to facilitate denial of updating the digital signature key pair on a per client basis.

4. (Delete)

5. (Once amended) The method of claim 1 further comprising the steps of:

determining a digital signature private key lifetime end date and a digital signature certificate creation date upon a user login to the public key system;

initiating, by a client unit, a digital signature key pair update request based on whether a difference between a current date and the digital signature private key lifetime end date (t1) is less than an absolute predetermined period of time and based on whether the difference between the current date and the digital signature private key lifetime end date (t1) is less than a selectable predetermined percentage of a total duration of a digital signature private key lifetime.

10. (Once Amended) The method of claim 9 wherein the step of providing selectable expiry data includes additionally providing updated digital signature key pairs, the step of storing includes storing a new digital signature key pair, and the step of associating also includes associating stored selected expiry data selected for the new digital signature key pair to affect a transition from an old digital signature key pair to a new digital signature key pair.

11. (Once Amended) The method of claim 10 wherein the selectable expiry data is digital signature certificate lifetime data for variably setting a lifetime end date for a digital signature certificate and also includes encryption certificate lifetime data for variably setting a lifetime end date for an encryption certificate associated with the given client.

14. (Six times amended): A system for providing updated digital signature key pairs to a plurality of clients in a public key system comprising:

multi-client management means for providing selectable digital signature expiry data to a plurality of clients and not by a client, including at least both public verification key expiry data and private signing key expiry data that are selectable on a per client basis wherein the digital signature key pairs are not shared among users;

means, accessible by the multi-client manager means, for digitally storing both selected public key expiry data and selected private key expiry data for association with a new digital signature key pair;

means, responsive to the stored selected public key expiry data, for associating the stored selected expiry data with the new digital signature key pair to affect a transition from an old digital signature key pair to a new digital signature key pair;

means for determining whether a digital signature key pair update request has been received from a client unit;

means for receiving a new digital signature key pair from the client unit in response to the digital signature key pair update request; and

wherein the means for associating the stored selected expiry data creates a new digital signature certificate containing the selected public key expiry data selected for the client that generated the digital signature key pair update request.

18. (Delete)

19. (Once amended) The system of claim 14 further comprising:

means for determining a digital signature private key lifetime end date and a digital signature certificate creation date upon a user login to the public key system;

client means for initiating a digital signature key pair update request based on whether a difference between a current date and the digital signature private key lifetime end date (t1) is less than an absolute predetermined period of time and based on whether the difference between the current date and the digital signature private key lifetime end date (t1) is less than a selectable predetermined percentage of a total duration of a digital signature private key lifetime.

21. (Six times amended): A storage medium comprising:

a stored program for execution by a processor wherein the program facilitates providing updated digital signature key pairs in a public key system by:

allowing entry of selectable expiry data for a plurality of clients and not through a client, including both at least public verification key expiry data and signing private key expiry data that are selectable on a per client basis wherein the digital signature key pairs are not shared among users;

digitally storing both selected public key expiry data and selected private key expiry data for association with a new digital signature key pair;

associating the stored selected expiry data with the new digital signature key pair to affect a transition from an old digital signature key pair to a new digital signature key pair;

determining whether a digital signature key pair update request has been received from a client unit;

receiving a new digital signature key pair from the client unit in response to the digital signature key pair update request; and

creating a new digital signature certificate containing the selected public key expiry data selected for the client that generated the digital signature key pair update request.

22. (Once Amended) The storage medium of claim 21 wherein the stored program allows selection of digital signature certificate lifetime data for variably setting a lifetime end date for a digital signature certificate.

23. (Once Amended) The storage medium of claim 21 wherein the stored program further includes affecting variable update privilege control on a per client basis by a multi-client manager unit to provide denial of updating the digital signature key pair on a per client basis.

24. (Delete)

25. The storage medium of claim 21 wherein the stored program further facilitates the steps of:

determining a digital signature private key lifetime end date and a digital signature certificate creation date upon a user login to the public key system;

initiating, by a client unit, a digital signature key pair update request based on whether a difference between a current date and the digital signature private key lifetime end date (t1) is less than an absolute predetermined period of time and based on whether the difference between the current date and the digital signature private key lifetime end date (t1) is less than a selectable predetermined percentage of a total duration of a digital signature private key lifetime.

26. The storage medium of claim 21 wherein the stored program provides a user interface to facilitate setting of the selectable expiry data to a desired state.

27. (New) The method of Claim 5 wherein the selectable predetermined percentage of a total duration of a digital signature private key lifetime includes a selectable period of time.

28. (New) The system of Claim 19 wherein the selectable predetermined percentage of a total duration of a digital signature private key lifetime includes a selectable period of time.

29. (New) The storage medium of Claim 25 wherein the selectable predetermined percentage of a total duration of a digital signature private key lifetime includes a selectable period of time.

30. A method for providing updated digital signature key pairs to a plurality of clients in a public key system comprising the steps of:

providing, by a multi-client manager unit and not by a client, selectable digital signature expiry data including at least public verification key expiry data, and selectable private signing key expiry data to a plurality of clients, that are selectable on a per client basis wherein the digital signature key pairs are not shared among users;

digitally storing both selected public key expiry data and selected private key expiry data for association with a new digital signature key pair;

[associating the stored selected expiry data with the new digital signature key pair to affect a transition from an old digital signature key pair to a new digital signature key pair; and]

determining whether a digital signature key pair update request has been received from a client unit;

receiving a new digital signature key pair from the client unit in response to the digital signature key pair update request;

associating the stored selected expiry data with the new digital signature key pair to affect a transition from an old digital signature key pair to a new digital signature key pair; and

wherein the step of associating the stored selected expiry data includes creating a new digital signature certificate containing the selected public key expiry data selected for the client generating the digital signature key pair update request, a user public key, a user name and a signature of the multi-client manager unit.